

**INFORMATION TECHNOLOGY SECURITY (ITS)  
MINIMUM BASELINE PROTECTIVE  
REQUIREMENTS**

<b>REQUIREMENTS</b>	<b>SENSITIVITY LEVEL 0</b>	<b>SENSITIVITY LEVEL 1 (All Level 0 Requirements Plus)</b>	<b>SENSITIVITY LEVEL 2 (All Level 0, And 1 Requirements Plus)</b>	<b>SENSITIVITY LEVEL 3 (All Level 0, 1, And 2 Requirements Plus)</b>	<b>CLASSIFIED (All Level 0, 1, 2, and 3 Requirements Plus)</b>
<b>ACCREDITATION</b>	<ul style="list-style-type: none"> <li>No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>Systems/networks evaluation yearly by the GSO; DAA accreditation not less than 1 year but not more than every 3 years.</li> </ul>
<b>AUDIT TRAIL</b>	<ul style="list-style-type: none"> <li>No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>Record all access failures to systems, files, objects, and resources.</li> <li>Record all systems privilege use</li> <li>Record all maintenance, software/hardware upgrades, and backups.</li> </ul>	<ul style="list-style-type: none"> <li>Audit records reviewed weekly.</li> <li>Audit records retained for 1 year.</li> <li>Conduct random unannounced reviews of system files.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0, 1 and 2.</li> </ul>	<ul style="list-style-type: none"> <li>Audit records for multi-level systems retained for 2 years.</li> </ul>
<b>AUTHORIZATION TO PROCESS</b>	<ul style="list-style-type: none"> <li>Management's written authorization to process <ul style="list-style-type: none"> <li>before operations begin</li> <li>after significant change.</li> </ul> </li> <li>Reauthorization every three years.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Level 0.</li> </ul>	<ul style="list-style-type: none"> <li>Reauthorization every two years.</li> </ul>	<ul style="list-style-type: none"> <li>Reauthorization annually.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0, 1, 2, and 3.</li> </ul>
<b>COMMUNICATIONS SECURITY (COMSEC)</b>	<ul style="list-style-type: none"> <li>No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>Data Encryption.</li> </ul>	<ul style="list-style-type: none"> <li>No uncontrolled dial-up access or unauthorized connections to external networks.</li> <li>Non-use of encryption must be justified.</li> </ul>	<ul style="list-style-type: none"> <li>Information, devices, or materials will be handled in compliance with NACSI 4005.</li> </ul>
<b>COMPUTER SECURITY AWARENESS TRAINING (CSAT)</b>	<ul style="list-style-type: none"> <li>Provide initial training to all new employees within 60 days of employment.</li> <li>Provide continuing training whenever there is: (1) A significant change in the ITS environment or procedures. (2) An employee enters a new position which deals with sensitive information.</li> <li>Conduct Refresher training as frequently as determined necessary based on the sensitivity of the information used or processed.</li> <li>Maintain signed acknowledgement of training for two years.</li> </ul>	<ul style="list-style-type: none"> <li>Conduct system or network-specific security training for users.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0 and 1.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0, 1 and 2.</li> </ul>	<ul style="list-style-type: none"> <li>Conduct mandatory computer security awareness training designed to enhance employees awareness of threat and vulnerabilities of ITS periodically.</li> </ul>

**INFORMATION TECHNOLOGY SECURITY (ITS)  
MINIMUM BASELINE PROTECTIVE  
REQUIREMENTS**

<b>REQUIREMENTS</b>	<b>SENSITIVITY LEVEL 0</b>	<b>SENSITIVITY LEVEL 1 (All Level 0 Requirements Plus)</b>	<b>SENSITIVITY LEVEL 2 (All Level 0, And 1 Requirements Plus)</b>	<b>SENSITIVITY LEVEL 3 (All Level 0, 1, And 2 Requirements Plus)</b>	<b>CLASSIFIED (All Level 0, 1, 2, and 3 Requirements Plus)</b>
<b>CONFIGURATION MANAGEMENT</b>	<ul style="list-style-type: none"> <li>• Maintain current hardware and software lists.</li> <li>• Maintain licenses for all software.</li> <li>• Maintain current network and system configuration diagrams.</li> </ul>	<ul style="list-style-type: none"> <li>• Maintain a process that controls changes to all sensitive software, hardware, or procedure in the system.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0 and 1.</li> </ul>	<ul style="list-style-type: none"> <li>• Controls must be in place that allow databases to be stored off-line.</li> </ul>	<ul style="list-style-type: none"> <li>• Security baseline changes must be approved by the DPI-ITSO or designee, and by division/site personnel before implementation.</li> </ul>
<b>CONTINGENCY PLAN/DISASTER RECOVERY</b>	<ul style="list-style-type: none"> <li>• No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>• Develop and document a plan that covers emergency response, recovery and return to normal operations.</li> <li>• Approval by Senior Management</li> <li>• Test, review and update annually.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0 and 1.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0, 1 and 2.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0, 1, 2 and 3.</li> </ul>
<b>DESTRUCTION OF INFORMATION TECHNOLOGY</b>	<ul style="list-style-type: none"> <li>• No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>• FOUO/SEB/Privacy Act/Proprietary or information identified as sensitive will be destroyed per established procedures</li> <li>• Shred diskettes after removing the outer protective casing.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0 and 1.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0, 1, and 2.</li> </ul>	<ul style="list-style-type: none"> <li>• The GSO will handle destruction of all classified materials at GSFC only. All other GSFC-operated sites contact the local security office for guidance on destruction procedures.</li> <li>• Destruction records must be retained for two years.</li> </ul>
<b>DISPOSAL OF INFORMATION TECHNOLOGY RESOURCES</b>	<ul style="list-style-type: none"> <li>• No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>• Remove sensitive information from fixed media prior to release: <ul style="list-style-type: none"> <li>- overwrite 3 times</li> <li>- degauss media</li> <li>- destroy media.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0 and 1.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0, 1, and 2.</li> </ul>	<ul style="list-style-type: none"> <li>• Media and memory declassification prior to removal from secure area.</li> </ul>
<b>DISPOSAL OF SENSITIVE INFORMATION</b>	<ul style="list-style-type: none"> <li>• Remove licensed software from fixed media.</li> <li>• Scan for viruses.</li> </ul>	<ul style="list-style-type: none"> <li>• Remove sensitive information from fixed media.</li> </ul>	<ul style="list-style-type: none"> <li>• Shred or deposit in a burn bag the following: <ul style="list-style-type: none"> <li>- Contractor Sensitive Data</li> <li>- Privacy Act Data</li> <li>- Proprietary Data</li> <li>- Procurement</li> <li>- Source Evaluation Board (SEB)</li> <li>- Risk Assessments.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• All Sensitivity Level 3 data in hardcopy form must be shredded or deposited in a burn bag.</li> </ul>	<ul style="list-style-type: none"> <li>• Media and memory declassification prior to removal from secure area.</li> </ul>
<b>ENVIRONMENTAL CONTROLS</b>	<ul style="list-style-type: none"> <li>• Install adequate dust, water, temperature, humidity and ventilation controls.</li> <li>• Install surge protection on all resources.</li> </ul>	<ul style="list-style-type: none"> <li>• Plastic sheeting to protect from overhead liquid discharge.</li> <li>• Humidity warning system.</li> <li>• Temperature warning system.</li> <li>• Water detectors under raised floor.</li> </ul>	<ul style="list-style-type: none"> <li>• UPS or Power Distribution Unit (PDU) for minicomputers, servers and mainframes.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0, 1 and 2.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0, 1, 2 and 3.</li> </ul>

**DRAFT**  
5/17/96

**INFORMATION TECHNOLOGY SECURITY (ITS)  
MINIMUM BASELINE PROTECTIVE  
REQUIREMENTS**

<b>REQUIREMENTS</b>	<b>SENSITIVITY LEVEL 0</b>	<b>SENSITIVITY LEVEL 1 (All Level 0 Requirements Plus)</b>	<b>SENSITIVITY LEVEL 2 (All Level 0, And 1 Requirements Plus)</b>	<b>SENSITIVITY LEVEL 3 (All Level 0, 1, And 2 Requirements Plus)</b>	<b>CLASSIFIED (All Level 0, 1, 2, and 3 Requirements Plus)</b>
<b>IDENTIFY SENSITIVITY LEVELS</b>	<ul style="list-style-type: none"> <li>No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>Assign a sensitivity level to each system, network, and application.</li> <li>Concurrence of DPI-ITSO required.</li> <li>DPI-ITSO maintains current inventory of DPI systems and networks.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0 and 1.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0, 1 and 2.</li> </ul>	<ul style="list-style-type: none"> <li>All systems that process classified information or are installed in a reconfiguration are Sensitive Level 3</li> </ul>
<b>INCIDENT REPORTING</b>	<ul style="list-style-type: none"> <li>Report security incidents to system or network manager, DPI-ITSO and NASA Automated Systems Incident Response Capability (NASIRC).</li> <li>Forward GSFC Form 24-10 (Incident/Investigative Report) to the DPI-ITSO and C-AISM.</li> </ul>	<ul style="list-style-type: none"> <li>Maintain a file of security incidents.</li> <li>Retain until the next Center ITS Security Review.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0 and 1.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0, 1 and 2.</li> </ul>	<ul style="list-style-type: none"> <li>Report incidents involving physical security, COMSEC, personnel security, COMPUSEC, INFOSEC, NRP STANDARDS, to the Technical Program Officer in the Goddard Security Office using GSFC Security Incident Report (March 1993).</li> </ul>
<b>LOGOFF AND TIMEOUT</b>	<ul style="list-style-type: none"> <li>No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>Suspend a user ID after 3 consecutive attempts.</li> </ul>	<ul style="list-style-type: none"> <li>Automatically log off or pause workstations or terminals that have not had keyboard activity for fixed period of time not to exceed 15 minutes.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0, 1, and 2.</li> </ul>	<ul style="list-style-type: none"> <li>Exceptions to log off workstations must be approved by 205.1.</li> </ul>
<b>LOGON BANNER</b>	<ul style="list-style-type: none"> <li>Install an Information Resources Oversight Committee (IROC) approved logon banner on each multi-user system and network reachable from another system or network.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Level 0.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0 and 1.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0, 1 and 2.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0, 1, 2 and 3.</li> </ul>
<b>MAINTENANCE AND REPAIR</b>	<ul style="list-style-type: none"> <li>Permission of the Property Custodian and a property pass to remove from Center.</li> <li>Remove licensed software from fixed storage media before property can be removed from Center.</li> </ul>	<ul style="list-style-type: none"> <li>Remove sensitive information from fixed storage media before property can be removed from Center.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0 and 1.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0, 1, and 2.</li> </ul>	<ul style="list-style-type: none"> <li>Permission of the Property Custodian and a property pass to remove from classified processing facility.</li> <li>Persons doing maintenance must be cleared and escorted and not allowed to access classified information.</li> <li>If maintenance personnel do not have a clearance, they must be escorted and not allowed access to classified information.</li> </ul>

**INFORMATION TECHNOLOGY SECURITY (ITS)  
MINIMUM BASELINE PROTECTIVE  
REQUIREMENTS**

<b>REQUIREMENTS</b>	<b>SENSITIVITY LEVEL 0</b>	<b>SENSITIVITY LEVEL 1 (All Level 0 Requirements Plus)</b>	<b>SENSITIVITY LEVEL 2 (All Level 0, And 1 Requirements Plus)</b>	<b>SENSITIVITY LEVEL 3 (All Level 0, 1, And 2 Requirements Plus)</b>	<b>CLASSIFIED (All Level 0, 1, 2, and 3 Requirements Plus)</b>
<b>MEDIA DECLASSIFICATION</b>	<ul style="list-style-type: none"> <li>• No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>• No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>• No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>• No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>• Prior to removal from secure area.</li> </ul>
<b>MEDIA AND MEMORY CLEARING</b>	<ul style="list-style-type: none"> <li>• No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>• No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>• No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>• No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>• All IT resources and equipment that incorporates read/write media must be cleared by over writing addressable locations, hardware memory reset, power off/on reset, or a combination of these measures.</li> </ul>
<b>MEDIA STORAGE</b>	<ul style="list-style-type: none"> <li>• Protect media from theft, vandalism, and natural disasters.</li> </ul>	<ul style="list-style-type: none"> <li>• Store media in an environmentally controlled area.</li> <li>• Ensure only authorized personnel can access the media.</li> <li>• Maintain an inventory accounting system for media entering and departing storage facility; verify inventory annually.</li> <li>• Identify all media with an external label and, when applicable, an internal label.</li> <li>• Provide a visual means of identification for all media containing Privacy Act Data, Proprietary Data and data marked as "For Official Use Only" (FOUO).</li> <li>• Ensure that magnetic media containing Privacy Act Data are degaussed or overwritten before being returned to use.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0 and 1.</li> </ul>	<ul style="list-style-type: none"> <li>• Verify media inventory semiannually.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0, 1, 2, and 3.</li> </ul>
<b>NETWORK AND SYSTEM ACCESS CONTROL</b>	<ul style="list-style-type: none"> <li>• Single user networked and multiuser computers and workstations must implement user identification (USERID).</li> <li>• Maintain log of all accesses to multi-user systems.</li> </ul>	<ul style="list-style-type: none"> <li>• Protective measures that ensure physical and/or logical control over authorization for and access to the system and processing resources.</li> <li>• When transferring files, error checking/correction software required.</li> </ul>	<ul style="list-style-type: none"> <li>• Protective measures that ensure identification and authorization of individual users; restriction of functional capabilities of individual users.</li> <li>• Written authorization for system interconnection.</li> </ul>	<ul style="list-style-type: none"> <li>• Controls that will at all times restrict and log individual user access by system resource, application and data files.</li> <li>• Authorization to access system resources, applications, and data files must be confirmed by the data owner (reconfirmation every 6 months).</li> </ul>	<ul style="list-style-type: none"> <li>• Mandatory access control based upon clearance levels and a Need-to-Know.</li> </ul>

**INFORMATION TECHNOLOGY SECURITY (ITS)  
MINIMUM BASELINE PROTECTIVE  
REQUIREMENTS**

<b>REQUIREMENTS</b>	<b>SENSITIVITY LEVEL 0</b>	<b>SENSITIVITY LEVEL 1 (All Level 0 Requirements Plus)</b>	<b>SENSITIVITY LEVEL 2 (All Level 0, And 1 Requirements Plus)</b>	<b>SENSITIVITY LEVEL 3 (All Level 0, 1, And 2 Requirements Plus)</b>	<b>CLASSIFIED (All Level 0, 1, 2, and 3 Requirements Plus)</b>
<b>NETWORK AND SYSTEM ADMINISTRATION</b>	<ul style="list-style-type: none"> <li>• Administrator assigned in writing.</li> </ul>	<ul style="list-style-type: none"> <li>• Maintain a complete inventory of system software and system application.</li> <li>• Develop rules of behavior for system/network users.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0 and 1.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0, 1, and 2.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0, 1, 2 and 3.</li> </ul>
<b>OPERATIONAL AND BACKUP SOFTWARE</b>		<ul style="list-style-type: none"> <li>• Bi-monthly full backup.</li> <li>• Incremental backups as determined by owner.</li> <li>• Most recent incremental backup stored on-site.</li> <li>• Other backup on-site storage in different building.</li> </ul>	<ul style="list-style-type: none"> <li>• Monthly full backup.</li> <li>• Weekly incremental backup.</li> <li>• On-site storage in different building.</li> </ul>	<ul style="list-style-type: none"> <li>• Weekly full backup.</li> <li>• Daily incremental backup.</li> <li>• Offsite storage of all backups except most recent incremental.</li> </ul>	<ul style="list-style-type: none"> <li>• Most recent incremental stored on site.</li> </ul>
<b>PASSWORD</b>	<ul style="list-style-type: none"> <li>• No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>• Minimum of 6 (preferably 8) alphanumeric characters.</li> <li>• Change at least every 180 days, upon termination of employment or reassignment of any person having knowledge of a system password, or whenever the password is suspected to have been compromised.</li> <li>• Are not to be displayed on the system monitor.</li> <li>• May not be any word appearing in an English or foreign dictionary.</li> <li>• Vendor provided and default passwords must be changed prior to system use.</li> <li>• Are not to be stored in batch files or keyboard macros.</li> <li>• Individual users are not to share, write down or electronically store passwords.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0 and 1.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0, 1, and 2.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0, 1, 2 and 3.</li> </ul>

**INFORMATION TECHNOLOGY SECURITY (ITS)  
MINIMUM BASELINE PROTECTIVE  
REQUIREMENTS**

<b>REQUIREMENTS</b>	<b>SENSITIVITY LEVEL 0</b>	<b>SENSITIVITY LEVEL 1 (All Level 0 Requirements Plus)</b>	<b>SENSITIVITY LEVEL 2 (All Level 0, And 1 Requirements Plus)</b>	<b>SENSITIVITY LEVEL 3 (All Level 0, 1, And 2 Requirements Plus)</b>	<b>CLASSIFIED (All Level 0, 1, 2, and 3 Requirements Plus)</b>
<b>PERSONNEL SECURITY</b>	<ul style="list-style-type: none"> <li>• No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>• Assign a position sensitivity rating to each Federal employee and each Non-Federal position.</li> <li>• Annual reevaluation of position sensitivity ratings.</li> <li>• Complete Foreign National Access Request for foreign national users of ITS resources prior to use.</li> <li>• National Agency Check (NAC) screening on all personnel who need access.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0 and 1.</li> </ul>	<ul style="list-style-type: none"> <li>• National Agency Check or National Agency Check with Inquiries and Credit Check (NACIC) depending on the position sensitivity rating.</li> </ul>	<ul style="list-style-type: none"> <li>• Federal employee <ul style="list-style-type: none"> <li>- NACIC for Secret</li> <li>- (SBI) for Top Secret.</li> </ul> </li> <li>• Non-Federal employee <ul style="list-style-type: none"> <li>- NAC for Secret</li> <li>- SBI for Top Secret.</li> </ul> </li> </ul>
<b>PHYSICAL SECURITY</b>	<ul style="list-style-type: none"> <li>• Annual unannounced fire drill.</li> <li>• Sprinkler system.</li> <li>• Smoke/heat detector.</li> <li>• Emergency power-off switch.</li> <li>• Annual inventory of hardware and software.</li> <li>• Secure hardware in locked area, lockable enclosure or use lockdown devices.</li> <li>• Secure portable computers in a locked area or container when not in use.</li> </ul>	<ul style="list-style-type: none"> <li>• Emergency powerdown procedure.</li> <li>• Change combination if someone who knows it leaves the organization.</li> <li>• Secure diskettes in a locked room or a lockable container.</li> <li>• Change combination if known by someone with unauthorized access.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0 and 1.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0, 1, and 2.</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Levels 0, 1, 2, and 3.</li> </ul>
<b>REPRODUCTION OF CLASSIFIED MATERIALS</b>	<ul style="list-style-type: none"> <li>• No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>• No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>• No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>• No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>• Machines must be approved by GSO.</li> <li>• A sign stating "Approved for Classified Reproduction" must be posted near the machine.</li> <li>• All waste copies must be placed in a burn bag and protected at the secret or confidential level.</li> <li>• To clear the copier, copy an unclassified printed page at least 4 times and handle the copies as classified waste.</li> </ul>

**INFORMATION TECHNOLOGY SECURITY (ITS)  
MINIMUM BASELINE PROTECTIVE  
REQUIREMENTS**

<b>REQUIREMENTS</b>	<b>SENSITIVITY LEVEL 0</b>	<b>SENSITIVITY LEVEL 1 (All Level 0 Requirements Plus)</b>	<b>SENSITIVITY LEVEL 2 (All Level 0, And 1 Requirements Plus)</b>	<b>SENSITIVITY LEVEL 3 (All Level 0, 1, And 2 Requirements Plus)</b>	<b>CLASSIFIED (All Level 0, 1, 2, and 3 Requirements Plus)</b>
<b>RISK MANAGEMENT PLAN</b>	<ul style="list-style-type: none"> <li>Implement a process to: (1) Measure risk (risk assessment)(2) Select appropriate controls to reduce risk to an acceptable level (risk mitigation), and (3) Document residual risk for management acceptance.</li> <li>Assess the risk <ul style="list-style-type: none"> <li>Before operation of new facility, system or network</li> <li>Upon significant change or every 5 years, whichever is sooner</li> </ul> </li> <li>Review and update the risk management plan every two years.</li> </ul>	<ul style="list-style-type: none"> <li>Review and update the risk management plan annually.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0 and 1.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0, 1 and 2.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0, 1, 2 and 3.</li> </ul>
<b>SECURITY PLAN</b>	<ul style="list-style-type: none"> <li>No Requirement.</li> </ul>	<ul style="list-style-type: none"> <li>Develop a Security Plan that meets the requirements of OMB CIR A-130, Appendix III.</li> <li>Review and update <ul style="list-style-type: none"> <li>Upon significant change</li> <li>Every three years.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Review and update every two years.</li> </ul>	<ul style="list-style-type: none"> <li>Review and update annually.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0, 1, 2, and 3.</li> </ul>
<b>SOFTWARE PROTECTION</b>	<ul style="list-style-type: none"> <li>Scan all software for malicious or unauthorized code prior to its installation.</li> <li>Anti-viral software installed on all file servers, microcomputers and portable computers.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Level 0.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0 and 1.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0, 1 and 2.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0, 1, 2, and 3.</li> </ul>
<b>USER RESPONSIBILITY STATEMENT</b>	<ul style="list-style-type: none"> <li>Provide system and network rules to each user.</li> </ul>	<ul style="list-style-type: none"> <li>Maintain a file of user responsibility statements for each account on the system and network.</li> <li>Reissue responsibility statement every three years.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0 and 1.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0, 1 and 2.</li> </ul>	<ul style="list-style-type: none"> <li>Same as Levels 0, 1, 2, and 3.</li> </ul>